УДК 004.9 **DOI: 10.18413/2518-1092-2020-5-3-0-6**

Ильинская Е.В.
Скрипина И.И.

АНАЛИЗ НАИБОЛЕЕ АКТУАЛЬНЫХ ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ОЦЕНКИ РИСКОВ ПРИ ПРОЕКТИРОВАНИИ ИНФОРМАЦИОННЫХ СИСТЕМ

Белгородский государственный национальный исследовательский университет, ул. Победы, д. 85, г. Белгород, 308015, Россия

e-mail: chmireva@bsu.edu.ru, skripina@bsu.edu.ru

Аннотация
В настоящее время проекты все более неопределенны уже на первых стадиях проектирования и сопровождаются большим количеством рисков. В статье рассматриваются инструментальные средства оценки рисков при проектировании информационных систем, такие как: CRAMM, RiskWatch и ГРИФ, проводится их краткое описание и сравнительный анализ. При проведении сравнительного анализа особое внимание уделяется следующим критериям: легкость работы для пользователя, стоимость лицензии за одно рабочее место, функциональность, функция ущерба.
Ключевые слова: риск при проектировании информационных систем; инструментальные средства оценки рисков; CRAMM; RiskWatch; ГРИФ.

UDC 004.9

Ilinskaja E.V.
Skripina I.I.

ANALYSIS OF THE MOST ACTUAL INSTRUMENTAL TOOLS FOR RISK ASSESSMENT IN DESIGNING INFORMATION SYSTEMS

Belgorod State National Research University, 85 Pobedy St., Belgorod, 308015, Russia

e-mail: chmireva@bsu.edu.ru, skripina@bsu.edu.ru

Abstract
Currently, projects are increasingly uncertain in the early stages of design and are accompanied by a large number of risks. The article discusses the tools for risk assessment in the design of information systems, such as: CRAMM, RiskWatch and GRIF, provides a brief description and comparative analysis. When conducting a comparative analysis, special attention is paid to the following criteria: ease of work for the user, the cost of a license for one workplace, functionality, damage function.
Keywords: risk in the design of information systems; risk assessment tools; CRAMM; RiskWatch; GRIF.

Проектирование информационных систем является очень долгосрочным и трудозатратным процессом, включающим в себя несколько этапов, который, как правило, связан с большим количеством сопутствующих рисков. В настоящее время проекты все более неопределенны уже на первых стадиях проектирования и сопровождаются большим количеством рисков.

В зависимости от сферы деятельности понятие «риск» может трактоваться по-разному, в этой связи существуют разные определения риска как категории. Обзор и анализ экономической литературы [3, 4], стандартов по управлению рисками [2] позволил сформулировать наиболее полный, на наш взгляд, подход к понятию «риск». Риск в проектной практике представляет собой вероятность возникновения неблагоприятных событий и их последствий, которые могут оказать влияние на успех реализации проекта и привести к возникновению финансовых потерь.

Рассмотрим наиболее актуальные инструментальные средства оценки рисков, которые могут быть использованы для оценки рисков при проектировании информационных систем:

- CRAMM;
- RiskWatch;
- Гриф.

Инструментальное средство CRAMM разработано британской компанией Insight Consulting [4].

Отличительной особенностью, характеризующей метод с положительной стороны, является системный комплексный подход, учитывающий количественную и качественную оценку рисков. При использовании инструментального средства CRAMM описываются защищаемые ресурсы с финансовой точки зрения в их денежном выражении, далее вычисляется необходимый показатель защиты проектируемой системы исходя из ценности защищаемой информации. На следующем шаге выполняется качественная и количественная оценка наступления рисковых событий для всех ресурсов, а также вычисляется уровень рисковых событий, далее применяются классические инструкции в зависимости от уровня рисковых событий и необходимого уровня защиты конкретного ресурса. В настоящее время пользователями инструментального средства CRAMM являются аудиторы со специальной подготовкой. Существует возможность использования богатой базы с готовыми примерами применения метода для множества ресурсов различных проектов.

Интерфейс инструментального средства CRAMM представлен на рисунке 1.

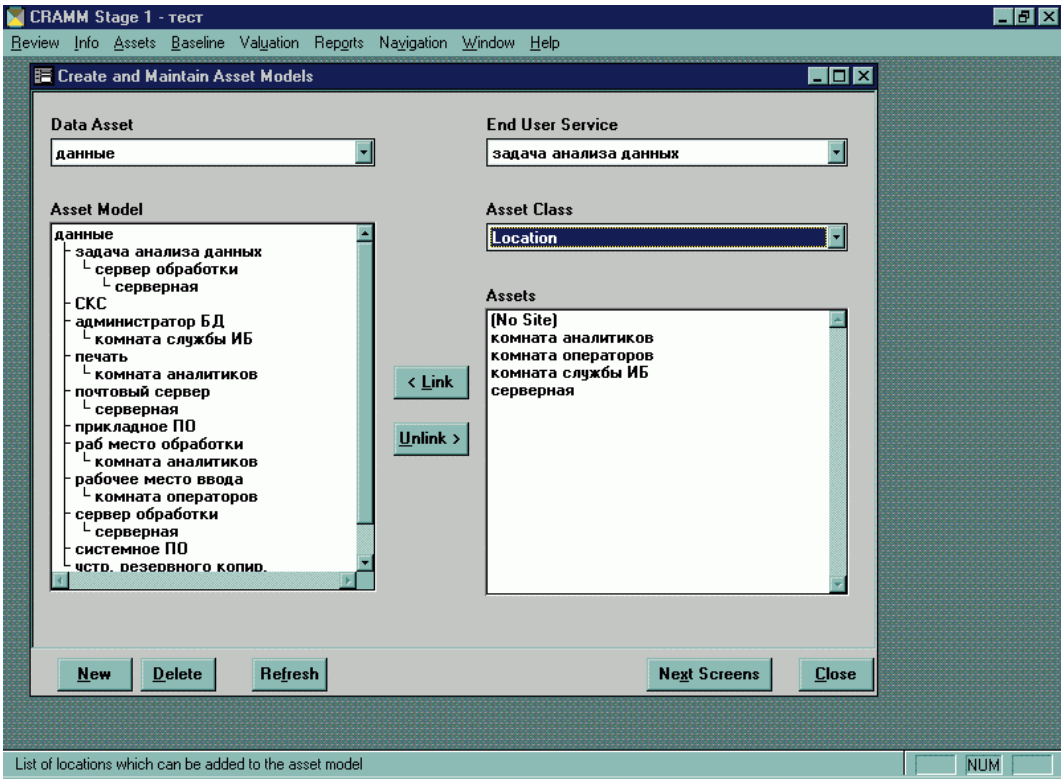

Рис. 1. Инструментальное средство CRAMM
Fig. 1. The CRAMM software tool

Рассмотрим недостатки инструментального средства CRAMM. Важным недостатком применения указанного средства является необходимость привлечения внешних аудиторов. Помимо этого, нужно учитывать, что инструментальное средство CRAMM применяется для проведения оценки рисков у уже внедренных информационных систем, а для оценки рисков при проектировании информационных систем он не предназначен. Инструментальное средство CRAMM разработано британской компанией и не маловажным недостатком является отсутствие русскоязычной версии данного средства.

Рассмотри инструментальное средство RiskWatch. Данное средство разработано компанией под названием RiskWatch Inc (США) для осуществления анализа и оценки различных видов рисков [5]. Отличительной чертой по сравнению с инструментальным средством CRAMM является ориентированность на идентификацию всех возможных рисков на первых стадиях проектирования информационной системы. Инструкции система выдает, опираясь на

утверждение, что финансовые затраты на управление возможными рисками не должны превышать сумму убытков от наступления какого-либо из идентифицированных рисков. На начальном этапе выявляются кластеры возможных рисков, далее просчитываются все возможные финансовые и другие убытки и классы неблагоприятных событий. Для достижения этой цели применяется специализированный опросник. Он содержит обширную базу данных с вопросами различных видов. В результате анализа ответов на вопросы опросника появляется возможность достаточно полно и четко идентифицировать риски, возникающие при проектировании информационной системы. На заключительном этапе выявляются взаимосвязи между убытками и рисковыми событиями. На основе полученных данных выполняется количественная оценка возможных убытков и генерируются инструкции по определенным мероприятиям предотвращения наступления риска.

Интерфейс инструментального средства RiskWatch представлен на рисунке 2.

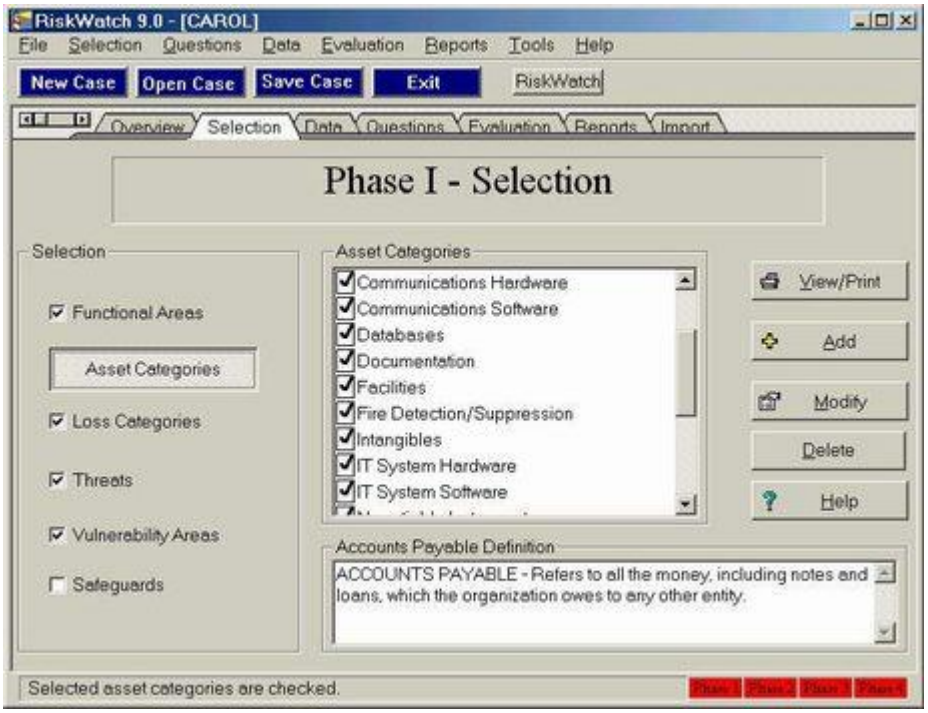

Рис. 2. Инструментальное средство RiskWatch
Fig. 2. The RiskWatch software tool

Использование инструментального средства RiskWatch позволяет количественно оценить вероятность наступления рисковых событий. На основе полученных результатов оценки можно судить о рентабельности проектирования и разработки информационной системы.

Инструментальное средство RiskWatch RiskWatch обладает некоторыми недостатками, в их числе: сложность проведения мониторинга, неинформативные инструкции по использованию информационных средств обеспечения защиты от наступления различных рисков, сложность, связанная с применением программы русскоязычными пользователями на английском языке.

Аналогом рассмотренных зарубежных инструментальных средств является отечественная русскоязычная программа ГРИФ (компания-разработчик Digital Security) [5]. В функционал программы входят анализ бизнес-процессов, оценка наступления возможных рисковых событий.

Инструментальное средство ГРИФ имеет интуитивно понятный для пользователя интерфейс, который представлен на рисунке 3.

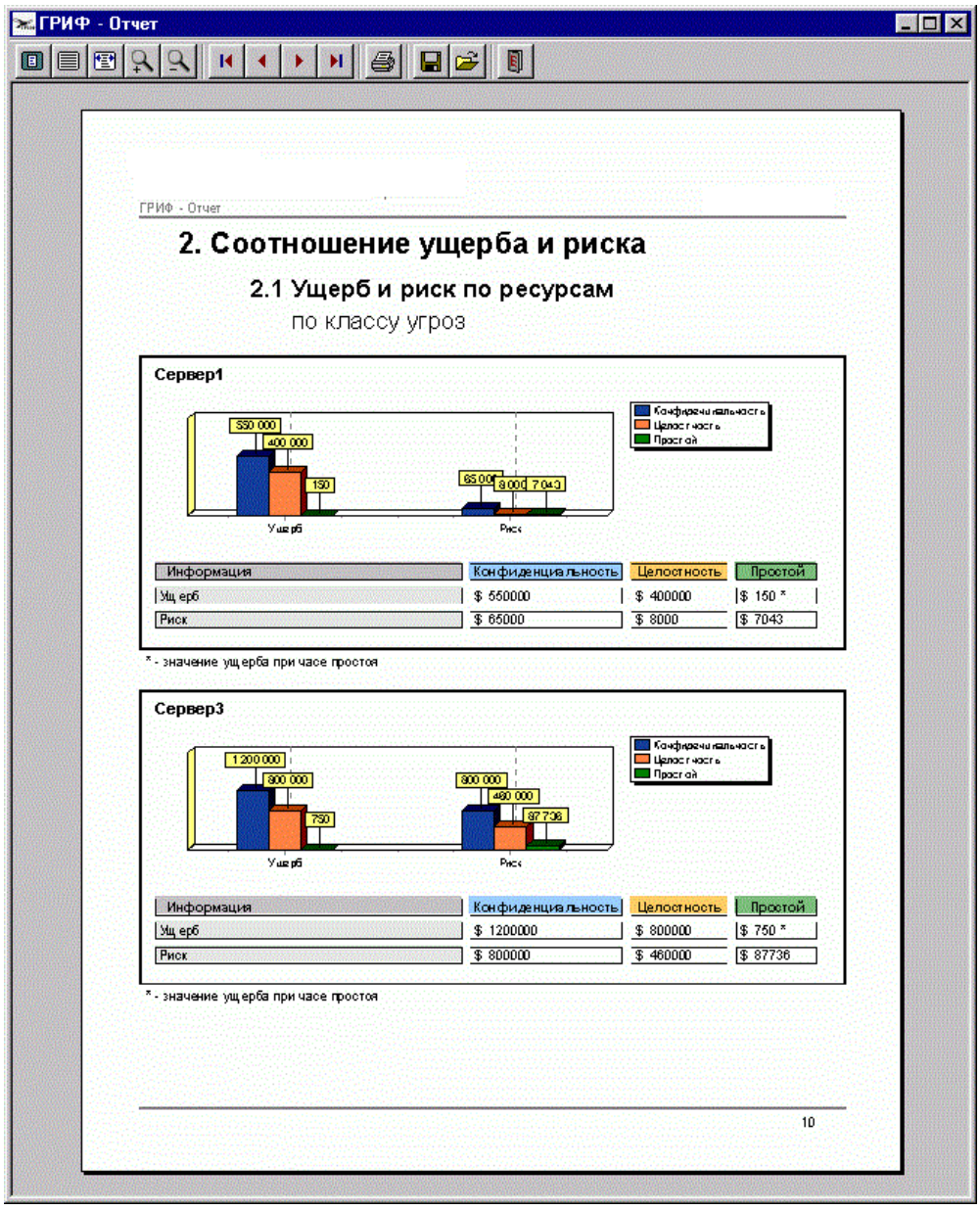

Рис. 3. Инструментальное средство ГРИФ
Fig. 3. The GRIF software tool

К достоинствам инструментального средства ГРИФ относят возможность анализа бизнес-процессов, на основе которого выполняется построение функциональной модели. Модель содержит описание информационных ресурсов, информацию о пользователях, а также сведения о средствах предотвращения наступления рисковых событий. С помощью инструментального средства ГРИФ на основе полученной модели выводится карта взаимосвязей пользователей и ресурсов в исследуемой информационной системе. На следующем этапе выполняется операция установления необходимости применения используемой политики безопасности в соответствии с архитектурой информационной системы. Выполняется это подобно тому, как и в инструментальном средстве RiskWatch, при помощи специализированных опросников с большой базой данных с вопросами. Далее производится анализ и оценка вероятности наступления рисковых событий. Выявляются все возможные угрозы и риски на каждом этапе жизненного цикла проекта. На основе полученных данных выполняется построение обновленной модели с применением математико-статистического моделирования. На завершающем этапе инструментальное средство выдает рекомендации по определенным мероприятиям предотвращения наступления риска.

Инструментальное средство ГРИФ обладает рядом достоинств и преимуществ по сравнению со своими аналогами, в их числе: мониторинг динамики бизнес-процессов, анализ политики безопасности в соответствии с архитектурой информационной системы. Есть и отрицательные черты у рассматриваемого средства, это небольшая база решений, что может повлиять на длительность и цену анализа рисков при проектировании информационных систем. Еще одним недостатком является необходимость обучения использования инструментального средства ГРИФ.

Сравнительные характеристики рассмотренных инструментальных средств приведены в таблице (таблица 1).

Таблица 1

Сравнительная характеристика инструментальных средств анализа рисков

Table 1

Comparative analysis of risk analysis tools

Критерии сравнения	**CRAMM**	**RiskWatch**	**ГРИФ**
Страна-разработчик	Великобритания	США	Россия
Наличие поддержки	+	+	+
Функционал	Входные данные: – ресурсы; – ценность ресурсов; – угрозы; – уязвимости системы; – выбор адекватных контрмер.	Входные данные: – тип информационной системы; – базовые требования в области безопасности; – ресурсы; – потери; – угрозы; – меры защиты.	Входные данные: – ресурсы; – сетевое оборудование; – виды информации; – группы пользователей; – средства защиты; – угрозы; – уязвимости.
Простота использования	-	-	+
Стоимость лицензии, $	От 2000 до 5000	От 10 000	От 1000
Метод оценки	Качественная оценка	Количественная оценка	Качественная и количественная оценки
Корпоративная версия	-	-	+
Задание ущерба	Как следствие нарушения свойств активов	Как следствие реализации угроз	Как следствие нарушения свойств активов
Функция ущерба	Для свойств доступности зависит от времени. Для свойств конфиденциальности целостности постоянна	Постоянна, не зависит от времени	Для свойств доступности зависит от времени. Для свойств конфиденциальност и целостности постоянна
Недостатки	1) Требует специализированных компетенций у пользователя. 2) Подходит для	1) Не учитывает организационный фактор. Оценка рисков, произведённая с	1) Нет возможности сравнения отчетов на разных этапах внедрения комплекса мер по

Критерии сравнения	CRAMM	RiskWatch	ГРИФ
	разработанных информационных систем, не учитывает особенности на этапе проектирования. 3) Огромное количество отчетов.	помощью инструментального средства, не является комплексной.	обеспечению защищенности 2) Отсутствие возможности добавления специфичных для разных сфер деятельности требований политики безопасности.

Проанализировав таблицу 1, можно сделать вывод, что среди рассмотренных инструментальных средств самым универсальным и подходящим под потребности российских пользователей является инструментальное средство ГРИФ. Оно позволяет проводить мониторинг динамики бизнес-процессов, анализ политики безопасности в соответствии с архитектурой информационной системы. У ГРИФ самая невысокая цена по сравнению с другими, оно не требуют наличия специализированных компетенций у пользователей, реализовано на русском языке.

Список литературы

1. Асадуллаев, Р.Г. Разработка средств оценки проектных рисков при создании информационных систем для сферы государственных услуг [Текст] / Р.Г. Асадуллаев, В.В. Ломакин, Н.П. Путивцева, О.С. Резниченко, Ю.Ю. Белоконь // Научно-технический вестник Поволжья, 2017. – № 5. – С. 120-122.

2. Воронцовский, А.В. Управление рисками: Учебник и практикум для бакалавриата и магистратуры [Текст] / А.В. Воронцовский. – Люберцы: Юрайт, 2016. – 414 с.

3. Домащенко, Д.В. Управление рисками в условиях финансовой нестабильности [Текст] / Д.В. Домащенко, Ю.Ю. Финогенова. – М.: Магистр, ИНФРА-М, 2010. – 238 с.

4. Гнедаш, Е.В. Метод CRAMM – комплексный подход к оценке рисков [Текст] / Е.В. Гнедаш // Информационные технологии в науке, управлении, социальной сфере и медицине: сборник научных трудов II Международной конференции «Информационные технологии в науке, управлении, социальной сфере и медицине» / под ред. О.Г. Берестневой, О.М. Гергет; Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2015. – С. 128-130.

5. Ильинская, Е.В. Методика оценки рисков при разработке автоматизированных информационных систем корпоративного уровня [Текст] / Е.В. Ильинская, В.В. Ломакин, Р.Г. Асадуллаев, Т.В. Зайцева // Научно-технический вестник Поволжья, 2018. – 11. – С. 218-223

6. Файзулаев, Д.Ф. Методы и средства анализа рисков информационной безопасности [Текст] / Д.Ф. Файзулаев // Безопасность информационных технологий, 2017. – Т. 24. – № 3. – С. 69-74.

References

1. Asadullaev, R.G. Development of means for assessing project risks in the creation of information systems for the sphere of public services [Text] / R.G. Asadullaev, V.V. Lomakin, N.P. Putivtseva, O.S. Reznichenko, Yu. Yu. Belokon // Scientific and technical bulletin of the Volga region, 2017. – No. 5. – Pp. 120-122.

2. Vorontsovsky, A.V. Risk Management: Textbook and Workshop for Bachelor's and Master's Degree [Text] / A.V. Vorontsovsky. – Lyubertsy: Yurayt, 2016. – 414 p.

3. Domashchenko, D.V. Risk management in conditions of financial instability [Text] / D.V. Domashchenko, Yu. Finogenova. – M.: Master, INFRA-M, 2010.- 238 p.

4. Gnedash, E.V. CRAMM method – an integrated approach to risk assessment [Text] / E.V. Gnedash // Information technologies in science, management, social sphere and medicine: collection of scientific papers of the II International conference "Information technologies in science, management, social sphere and medicine" / ed. O.G. Berestneva, O.M. Gerget; Tomsk Polytechnic University. – Tomsk: Publishing house of the Tomsk Polytechnic University, 2015. – Pp. 128-130.

5. Ilyinskaya, E.V. Methodology for assessing risks in the development of automated information systems at a corporate level [Text] / E.V. Ilyinskaya, V.V. Lomakin, R.G. Asadullaev, T.V. Zaitseva // Scientific and technical bulletin of the Volga region, 2018. – 11. – Pp. 218-223

6. Fayzulaev, D.F. Methods and tools for the analysis of information security risks [Text] / D.F. Faizulayev // Security of information technologies, 2017. – T. 24. – No. 3. – P. 69-74.

Ильинская Елена Владимировна, кандидат экономических наук, доцент кафедры прикладной информатики и информационных технологий
Скрипина Ирина Ивановна, старший преподаватель кафедры прикладной информатики и информационных технологий

Ilinskaja Elena Vladimirovna, Candidate of Economic Science, Docent of the Department of Applied Informatics and Information Technology
Skripina Irina Ivanovna, Senior Lecturer of the Department of Applied Informatics and Information Technologies